



TRAVEL SAFETY AND SECURITY TIPS
SDPD Neighborhood Policing Resource Team
April 9, 2013

CONTENTS

PERSONAL SAFETY AND SECURITY

When Away from Home
In a Hotel or Motel
When Using an ATM
While Driving
On a Cruise
Avoiding Terrorists

PROPERTY SECURITY

Protecting Your Home and Property When You Are Away
Credit Freeze and Use of Credit Cards
At a Hotel or Motel
When Out Carrying a Purse or Wallet
What to Do If Your Purse or Wallet is Lost or Stolen
Using Wi-Fi, Laptops, and Mobile Devices in Public Places
In Your Vehicle

The tips in this paper will help you protect yourself and your property when you are travelling away from home. Additional tips on home security, vehicle security, and preventing fraud and identity theft are available on the SDPD website at www.sandiego.gov/police/services/prevention/tips/index.shtml.

PERSONAL SAFETY AND SECURITY

When Away from Home

- Travel with a friend or in a group when possible. There is safety in numbers.
- Plan your touring. Don't discuss your plans with strangers. Beware of strangers who seem overly anxious to help you. Select guides carefully.
- Get good directions to avoid getting lost.
- Find an open business to get directions if you get lost. Don't appear to be lost by stopping and looking at addresses or street signs.
- Stick to well-lighted main streets and public areas.
- Leave your itinerary with a friend or relative and check in with them periodically.
- Keep track of time and don't be late for appointments or meetings.
- Shop with a friend when possible.
- Don't buy things from people on the street who offer you a great deal, especially if you have to follow them somewhere to get it.
- Don't fight for your purse if someone tries to take it by force.
- Before getting into a cab note the cab number and driver's name.

In a Hotel or Motel

- If the desk clerk says your room number aloud when you check in, ask for a different room and have the number written on your keycard sleeve and discreetly handed to you.
- Avoid rooms with ground-floor windows or sliding-glass doors to pools or beach areas.
- If you feel uncomfortable walking to your room alone, ask the desk clerk to provide an escort.
- Determine the most direct route to and from your room, to fire escapes, stairs, elevators, and phones. Count the number of doors between your room and the exits in case you need to escape in smoke or darkness.
- Keep your door locked when you are in your room. Use both the deadbolt lock and the security bar/chain.
- Keep your windows locked, and blinds and drapes closed for privacy.
- Be sure that sliding glass doors and doors to connecting rooms are locked.
- Safeguard your room key or card at all times.
- Use the peephole in the door to identify anyone requesting entry. Open the door only if you are certain it is safe to do so.
- If you are worried about being spied on through the peephole in the door cover it with a piece of opaque tape.
- If you haven't requested room service or housekeeping and someone knocks on your door claiming to be a staff member, call the front desk to verify the claim before opening the door.
- If you receive a call about an emergency that requires you to leave your room, hang up and call the front desk to verify it.
- If you receive a call asking for your credit card number to verify a room charge, hang up. It's probably a scam. Call the front desk to see if there's any problem with your account.
- Report any suspicious persons or activities to the front desk.
- Don't stay in a ground-floor room or rooms near stairwells or elevators, especially if you are a woman and traveling alone.
- Don't leave anything on your door knob to indicate that you are not in your room. Call housekeeping to request maid service. Call room service to order food.
- Use valet parking if the garage is dimly lit or the neighborhood has a high crime rate.
- Ask your hotel concierge or desk clerk about dangerous areas and avoid them. Neighborhoods can change a new threats may have emerged since the last time you visited or the guidebook you're using was printed.
- When you go out tell the hotel manager when you expect to return and who to call if you're not back by then.
- Carry a card with your hotel's name, address, and phone number.

When Using an ATM

- Use ATMs that are inside a store or a bank. If you use an outside ATM, it should be well-lighted, in a busy area, under video surveillance, and have clear lines of sight in all directions, i.e., there should be no nearby building corners, shrubs, signs, etc. that could provide possible hiding places for an attacker.
- Get off your cell phone and be alert when using an ATM.
- Cover the PIN entry and cash output as much as possible.
- Be aware of your surroundings before and during your transaction, especially between dusk and dawn. Return later or use an ATM in a store or bank if you notice anything suspicious, e.g., a person loitering nearby.
- Complete your transaction as fast as possible and leave the facility.
- Don't go alone.
- Park in a well-lighted area as close to the ATM as possible.
- Keep your doors locked and passenger and rear windows rolled up when using a drive-through ATM.
- Put your cash, receipt, and ATM card away promptly. Count your cash later in private. Do not leave your receipt at the ATM site.
- Avoid being too regular. Don't use the same ATM at the same time of day and day of the week.
- Make sure you are not being followed when you leave an ATM location. Drive immediately to a police or fire station, or any well-lighted and crowded location or open business and get help if you are being followed. Flash your lights and sound your horn to attract attention.
- Give up your money or valuables if you are confronted by an armed robber. Any delay can make a robber more nervous and increases the likelihood of violence.

While Driving

- Keep your doors locked and your windows closed.
- Know where you are going. Stop and get directions before you get lost.
- Do not stop to assist a stranded motorist. Call or drive to the nearest phone and report the situation.
- Drive to the nearest open business and call the police if anyone is following you.
- Honk your horn or flash your lights to attract attention if you are threatened.
- Keep enough gas in the tank so you won't run out.
- If your vehicle breaks down or runs out of gas, pull over to the right as far as possible, raise the hood, and call or wait for help. Remain in your vehicle with the doors and windows locked until you can identify any person who comes to help.

On a Cruise

- Be skeptical. Don't assume you can trust other passengers. Criminals travel too.
- Stay sober. Don't let alcohol impair your judgment. Only drink beverages you have seen prepared. Ask that bottled drinks be served unopened.
- Set rules for your children and keep an eye on them. Make sure they don't drink. Report any crew members who serve alcohol to minors.
- Meet fellow passengers in public areas, not cabins.
- Use all locks on your cabin door. Never open it to a stranger.
- When you enter your cabin check the bathroom and closet before closing the door.
- Don't socialize with the crew. Make sure your children know that crew areas are off limits.
- Dress down. Leave expensive jewelry and watches at home. They only make you a target for thieves.
- Lock all valuables in a safe and guard your key card as you would a credit card.
- Don't stand or sit on the ship's railing.
- Never go to any isolated areas of the ship alone, especially in the evening and early morning.
- Know where the members of your party are at all times. Report a missing person immediately.
- Attend the ship safety drills and learn its emergency procedures.
- Bring phone numbers of U.S. embassies or consulates in the cities on your itinerary so you can contact them if a problem arises. You can get them online at **www.usembassy.gov**.
- If you are a victim of a crime at sea call the FBI at **(202) 324-3000** from the ship to report the crime. Call the U.S. embassy or consulate if you are a victim of a crime on shore. Take photos of the crime scene and any injuries you suffered. Get the names, addresses, and phone numbers of possible witnesses. Take statements. Don't expect the cruise line to take physical evidence. Also notify your family, doctors, lawyers, insurance companies, etc. as appropriate.

Avoiding Terrorists

- Before you leave go the U.S. Department of State website **www.travel.state.gov** to check Travel Alerts and Travel Warnings.
- Avoid large chain hotels or ones near U.S. embassies or consulates, landmarks, religious centers, or places where demonstrations have occurred. Choose a small hotel in a quiet neighborhood.
- Consider the following in choosing a hotel and reserving a room.
 - Has its staff had security and emergency management training in the past year?
 - Does it have an emergency evacuation plan?
 - Are background checks done on all members of its staff?
 - Are there sprinklers in every room?
 - Is security on duty 24/7?
 - Does it have electronic key-card access? Do its elevators require key cards?
 - If rooms are directly over the lobby, reserve a room located between the third and seventh floors. They are within reach of most fire-department ladders.
- Do the following if you are trapped in your hotel by armed assailants:
 - Double-lock your door and barricade it with heavy furniture.
 - Drag a mattress to the center of the room and hunker down under it.

- Stuff wet towels under the door if there is smoke.
- Keep quiet so you don't alert attackers to your presence.
- Avoid windows, a blast outside can be lethal.
- Visit major attractions at less-busy hours.
- Avoid restaurants and clubs frequented by Americans.
- Don't wear clothes that advertise your nationality.
- Register with the nearest American embassy or consulate or do it online at <https://travelregistration.state.gov> so you can be contacted in the event of a crisis or emergency.

PROPERTY SECURITY

Protecting Your Home and Property When You Are Away

- Lock all doors and windows. Use deadbolts, dowels, or locking pins in sliding glass doors and windows to keep them from being pried open.
- Leave window blinds and curtains in their normal daytime positions without exposing any valuable items.
- Never announce your travel plans or whereabouts on Facebook, Twitter, or other social networking sites. In a 2011 survey of 50 convicted burglars in the United Kingdom, 40 said that social media was being used to identify properties with absent owners.
- Wait until you get home to post your travel blog and photos. Remove geotags with a metadata removal tool if you publish photos on the Internet while you are away. Even better, turn off the geotagging feature on your smartphone.
- Use timers on lights, radios, TVs, etc. to make them go on and off during the day and night to make your home appear occupied.
- Stop mail delivery, or have a neighbor pick it up. (This also helps to prevent identity theft.)
- Stop newspaper delivery or have neighbor pick them up. Also have neighbor pick up anything left at your door, on your driveway, or elsewhere.
- Keep grass watered and cut. Water and trim other landscaping.
- Ask the neighbors to watch your home and report any suspicious activities.
- Invite a neighbor or family member of park a vehicle in your driveway.
- Leave your itinerary with a neighbor so you can be contacted in an emergency.
- Disconnect your electric garage door opener and padlock the door, preferably on the inside.
- Lock or otherwise secure all pet doors that a person might crawl through.
- Visit your local SDPD Area Station to request home checks when you'll be out of town. Their addresses and phone numbers are at the end of this paper. Call first to make sure the front counter is open.
- Set your burglar alarm and notify your alarm company that you will be away. Then if an alarm occurs when you are away the company will not call your home first to verify the alarm; it will notify the police directly. Also provide the alarm company with an up-to-date list of persons to contact about the alarm and the need to secure your home after a burglary.
- If you have a house or pet sitter, familiarize that person with your home's security systems and procedures and stress the importance of following them.

Credit Freeze and Use of Credit Cards

- Consider placing a security freeze on your credit reports. Go to the websites of Equifax, Experian, and TransUnion for their procedures and fees for placing and lifting freezes. Their addresses are: www.equifax.com, www.experian.com, and www.transunion.com, respectively. A freeze will stop these reporting companies from sharing your credit reports with any creditors or insurance companies. Thus anyone who might have stolen your identity will be unable to open new accounts in your name while you are gone because creditors will usually not open new accounts without credit reports. You can lift the freeze when you return.
- Take only essential credit cards. Leave debit cards at home in a secure place.
- Alert your credit card companies about when, where, and how long you will be away. This will enable their fraud departments to stop charges if your card is used where you are not, and reduces the risk that charges made where you are going to be will not be accepted.

- Consider using Virtual Account Numbers (VANs) for your credit cards. They offer one-time use and are disposable. Some credit card companies offer them. Here's how they work. Log onto your credit card account and generate random account numbers. Enter them on a merchant's bill instead of your real account number. This VAN will only be valid for the time it takes the merchant to process your transaction. Your credit card company will recognize it and charge the amount to your account. If a hacker breaks into the merchant computer and steals your VAN, it will be useless. Note that VANs cannot be used for purchases that require you to show your credit card because the account numbers won't match. VANs make it virtually impossible for anyone to steal your real account number from a merchant. A variant on the VAN is a temporary card number that has a spending limit, expiration date, and security code that you can use for multiple transactions.
- Inform your credit card companies when you return and review transactions for the period you were gone. Continue to monitor your personal financial account transactions for unauthorized or unapproved use.

At a Hotel or Motel

- Use all available locks on the doors and windows.
- Make sure the door is securely locked when you leave your room.
- Unpack and place your belongings in the closet and dresser. Arrange things so you can easily tell if something is missing. Keep a list of all things you brought from home.
- Lock your suitcases so they cannot be used to carry things out. Consider hiding electric appliances and other valuable items in your suitcase.
- Don't leave cash, checks, credit cards, jewelry, vehicle keys, etc. in the room. Take them with you or lock them in the hotel safe.
- Report any lost or stolen items to the hotel management as well as to the police.
- Don't use hotel computers for anything that requires passwords or personal information. You never know if any identity-stealing software is installed.
- Never give out any personal information to someone who calls and says he or she is at the front desk and needs the information. Ignore the request and go to the desk yourself to see if any information is needed.

When Out Carrying a Purse or Wallet

- Carry only a driver's license, a minimum amount of cash, traveler's checks, a credit card, and insurance cards. Don't carry blank checks or a checkbook. Don't carry anything with PINs, account numbers, or passwords written on it. And don't carry a debit card.
- Don't carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card in a safe place at home and bring it if needed for a doctor appointment.
- Make a list of all the cards you carry. Include all account numbers and phone numbers to call to report a lost or stolen card. Also make photocopies of both sides of all the cards. (If you carry a library card, make a copy of it too.) Keep the list and copies in a safe place at home. Also bring copies to put in your hotel safe along with copies of your passport, tickets, traveler's check numbers, an extra credit card, and other important papers.
- Don't carry personal information of your family members.
- It's better to leave anything you don't need at home.
- Avoid carrying a purse if possible. Wear a money pouch instead.
- Carry a purse with a shoulder strap if you must. Keep the strap over your shoulder, the flap next to your body, and your hand on the strap. Hang the purse diagonally across your body.
- When wearing a coat and carrying a purse, conceal the strap and purse under the coat.
- Keep a tight grip on your purse. Don't let it hang loose or leave it on a counter in a store.
- Carry your wallet, keys, and other valuables in an inside or front pants pocket, a fanny pack, or other safe place. Don't carry a wallet in a back pocket.
- If you have an empty pocket, carry a spare wallet you can give to a robber. Put a few dollars, an expired credit card, and an old hotel key card in it.
- Never put your purse or wallet on a counter while shopping.
- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet

and are essentially useless in stealing the information on your card. And even if that information is “hi-jacked,” the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information on the chip is not the same as that on the magnetic strip, and it cannot be used to create a functioning counterfeit version of the card. If you have a card with a RFID chip and don’t want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.

- Since August 2007 all passports issued by the U.S. State Department have a small contactless RFID computer chip embedded in the back cover. They are called “Electronic or e-passports.” The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder, a unique chip identification number, and a digital signature to protect the stored data from alteration. Unauthorized reading of e-passports is prevented by the addition of a radio-frequency blocking material to their covers. The passports cannot be read until they are physically opened. Then there are protocols for setting up a secure communication channel and a pair of secret cryptographic keys in the chip to ensure that only authorized RFID readers can read the data on the chip.
- In July 2008 the U.S. State Department began issuing U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive than a passport book. It cannot be used for international travel by air. To increase speed, efficiency, and security at U.S. land and sea border crossings the card contains a RFID chip. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the card when it is not in use. Make sure you carry the card in the sleeve.

What to Do If Your Purse or Wallet Is Lost or Stolen

- File a police report in the jurisdiction where your wallet was lost or stolen. Also file one in the jurisdiction where you live. Get a copy of the report. You may need to send copies elsewhere.
- Report the loss to one of the three Consumer Credit Reporting Bureaus (CCRBs). Also contact one of the CCRBs to have an initial fraud alert placed on your credit reports. Their phone numbers are: **(800) 525-6285** for Equifax, **(888) 397-3742** for Experian, and **(800) 680-7289** for TransUnion. The CCRB you call is required to notify the other two. Ask to have a fraud alert placed on your credit reports. It will tell creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. In placing a fraud alert you will be entitled to free copies of your credit report from each CCRB. Order them a few weeks after your loss and review them carefully. Look for inquiries from companies you haven’t contacted, accounts you didn’t open, and debts on your accounts that you can’t explain. Fraud alerts are good for 90 days and can be renewed. They are free. This alert may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts.
- Alert your banks of the loss and request new account numbers, checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the loss.
- Call your credit card companies and request account number changes. Don’t ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new number issued so your old numbers will not show up as being “cancelled by consumer” on your credit reports.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the loss. If you still want a charge account, request a new number.
- Contact the IRS if your Social Security card or any other card with your SSN on it was in your purse or wallet. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. Call its Identity Theft toll-free line at **(800) 908-4490**. Also contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at **www.ssa.gov/org**.
- Call the SSA at **(800) 325-0778** if your Medicare card is lost or stolen. And ask for a replacement.
- If your driver license was lost, contact the California DMV Fraud Hotline at **(866) 658-5758** to report the loss, request a replacement license, ask that a stolen/lost warning be placed in your file, and check that another license has not been issued in your name.

- If your library card was lost, contact the library immediately. Otherwise you could be held financially responsible for any material borrowed after the loss.
- If your automobile, homeowners, or health insurance cards were lost, notify the companies ask request replacements.
- If your passport was lost or stolen in the United States, report it to the U. S. Department of State by calling (877) 487-2778. Operators are available from 8 a.m. to 10 p.m. ET, weekdays excluding Federal holidays. Or you complete, sign, and submit Form DS-64, Statement Regarding a Lost or Stolen Passport, to the U. S. Department of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St. NW, Ste. 500, Washington DC 20036. If it was lost or stolen overseas contact the nearest U. S. Embassy or Consulate.
- To replace a lost or stolen passport in the United States submit Forms DS-11, Application for a U. S. Passport and DS-64 in person at a Passport Agency or Acceptance Facility. If you are overseas, go to the nearest U. S. Embassy or Consulate if you are overseas to replace it.

Using Wi-Fi, Laptops, and Mobile Devices in Public Places

The following tips are provided by the U.S. Department of Homeland Security's Transportation Security Administration.

- Be aware that using Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places poses major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure.
- Also be aware that unsecure laptops and mobile devices like smartphones make it easy for a hacker to intercept information to and from the web, including passwords and credit- or debit-card numbers. They are also vulnerable to virus and spyware infections, and to having their contents stolen or destroyed.
- Install the latest operating system in your mobile devices and download all security software updates into your laptops. This will protect you from current viruses, worms, spyware, Trojan horses, spam, and other dangerous malware.
- Before you connect to any public Wi-Fi in a hotel, airport, train/bus station, café, or other place you should confirm the name of the network and its login procedures with an appropriate person to ensure that the network is legitimate.
- Don't use public Wi-Fi to perform sensitive transactions such as banking and online purchases.
- Always check your surroundings in public places to ensure that no one can view sensitive information on your screen or the keys you use to enter information.
- Never leave your mobile devices, including any USB/external storage devices, unattended in a public place. And if you plan to leave them in your hotel room, make sure they are appropriately secured.
- Make sure you take your mobile devices, including any USB/external storage devices, with you when you leave a public place.
- Turn off a Bluetooth-enabled device when it is not in use to prevent someone from connecting to your device and gaining access to your sensitive information.
- Never connect your mobile devices to any public charging station to prevent malicious software from being installed and/or access to your sensitive information.
- See the SDPD Cyber Security paper at www.sandiego.gov/police/pdf/crimeprevention/CyberSecurity.pdf for steps to take to reduce these risks.

In Your Vehicle

- Lock packages and other valuables in the trunk before you park, never after you park. Don't put packages in your vehicle and then return to stores for more shopping. Thieves may be watching.
- Park in open, well-lighted, and populated areas near your destination. In a garage park where you don't have to use stairs or elevators. Never park next to trucks, vans, dumpsters, and other objects that obstruct visibility and provide hiding places. Check that no one is near your vehicle before you get out.
- Avoid parking or walking near strangers loitering or sitting in vehicles.
- Lock your vehicle, and make sure the windows are closed and nothing of value is in sight.
- Conceal maps or travel brochures that might indicate you are a tourist.

- Remember where you parked so you can return directly to your vehicle. Be alert and walk away purposefully.
- Check that no one is hiding in or around your vehicle before you get in. If a van has parked next to your vehicle, enter on the other side.
- Lock the doors immediately after getting in your vehicle.
- Don't resist or argue with a carjacker. Your life is much more valuable than your vehicle.

SDPD AREA STATIONS

Central	2501 Imperial Ave. SD 92102	(619) 744-9500
Eastern	9225 Aero Dr. SD 92123	(858) 495-7900
Mid-City	4310 Landis St. SD 92105	(619) 516-3000
Northeastern	13396 Salmon River Rd. SD 92129	(858) 538-8000
Northern	4275 Eastgate Mall SD 92037	(858) 552-1700
Northwestern	12592 El Camino Real SD 92130	(858) 523-7000
Southeastern	7222 Skyline Dr. SD 92114	(619) 527-3500
Southern	1120 27th St. SD 92154	(619) 424-0400
Western	5215 Gaines St. SD 92110	(619) 692-4800